Primary Elements in Cyclotomic Fields with Applications to Power Residue Symbols, and More

Éric Brier[1], Rémi Géraud-Stewart[2], Marc Joye[3], David Naccache[4]

[1]Malissard, France
[2]Qualcomm, San Diego, CA, USA
[3]Zama, Paris, France
[4]École normale supérieure, Paris, France

Abstract *Higher-order power residues have enabled the construction of numerous public-key encryption schemes, authentication schemes, and digital signatures. Their explicit characterization is however challenging; an algorithm of Caranay and Scheidler computes p^{th} power residue symbols, with $p \leqslant 13$ an odd prime, provided that primary elements in the corresponding cyclotomic field can be efficiently found.*
In this paper, we describe a new, generic algorithm to compute primary elements in cyclotomic fields; which we apply for $p = 3, 5, 7, 11, 13$. A key insight is a careful selection of fundamental units as put forward by Dénes. This solves an essential step in the Caranay–Scheidler algorithm. We give a unified view of the problem. Finally, we provide the first efficient deterministic algorithm for the computation of the 9^{th} and 16^{th} power residue symbols.

1 MOTIVATION

Quadratic residues played a central role in building the first provably secure public-key cryptosystems [10]. A number is a quadratic residue modulo n when it can be expressed as the square of an integer modulo n, although that integer may be hard to find. This notion, along with generalizations to higher powers (called *higher-order power residues*), have enabled the construction of numerous public-key encryption schemes, authentication schemes, and digital signatures [26, 21, 22, 1, 2, 18].

The computation of p^{th} power residue symbols, when p is an odd prime $\leqslant 13$, can be performed by a generic algorithm of Caranay and Scheidler [4, § 7], although the concrete implementation for a given p remains challenging (see, e.g., [12] for the 11^{th} power residue symbol and [3] for the 13^{th} power residue symbol). The computation of the 4^{th} power residue symbol [25, 7] and of the 8^{th} power residue symbol [15, Chap. 9] (see also [11]) was solved independently. Finally, a generic algorithm was proposed by de Boer and Pagano [8], but it is inherently a *probabilistic* method which makes it unusable in most cryptographic settings. This leaves open the question to deterministically compute 9^{th} residue symbols, and all power residue symbols above the 13^{th}.

In this paper, we provide a unified and simplified approach to compute primary elements in cyclotomic fields, encompassing all previously-known results. This makes the Caranay–Scheidler algorithm practical, as it fundamentally relies on the (hitherto specialized) determination of primary elements. We also describe efficient deterministic algorithms for computing the 9^{th} and 16^{th} power residue symbols, which were open problems.

2 DEFINITIONS AND NOTATION

Throughout this paper, unless otherwise specified, $p \leqslant 13$ denotes an odd rational prime.

Let $\zeta := \zeta_p = e^{2\pi i/p}$ be a primitive p^{th} of unity and let $\omega = 1 - \zeta$. The ring of integers in the cyclotomic field $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$. It is known to be *norm-Euclidean* [16, 14]; in particular, $\mathbb{Z}[\zeta]$ is a unique factorization domain. Two elements α and β of $\mathbb{Z}[\zeta]$ are called *associates* if they differ only by a unit factor. We write $\alpha \sim \beta \iff \exists \upsilon \in \mathbb{Z}[\zeta]^\times$ such that $\alpha = \upsilon\beta$. The element ω is a prime in $\mathbb{Z}[\zeta]$ above p; we have $\omega^{p-1} \sim p$.

Since ζ is a root of the p^{th} cyclotomic polynomial, $\Phi_p(z) = z^{p-1} + \cdots + z + 1$, any algebraic integer $\alpha \in \mathbb{Z}[\zeta]$ can be expressed as

$$\alpha = \sum_{j=0}^{p-2} a_j\, \zeta^j \quad \text{with } a_j \in \mathbb{Z} \ .$$

The powers ω^k with $0 \leqslant k \leqslant p-2$ also form an integral basis of $\mathbb{Q}(\zeta)$. Given $\alpha = \sum_{j=0}^{p-2} a_j\,\zeta^j$, an application of the binomial theorem leads to

$$\begin{aligned}\alpha &= \sum_{j=0}^{p-2} a_j\,\zeta^j = \sum_{j=0}^{p-2} a_j\,(1-\omega)^j = \sum_{j=0}^{p-2} a_j \sum_{k=0}^{j} \binom{j}{k}(-\omega)^k = \sum_{k=0}^{p-2}\sum_{j=k}^{p-2} a_j \binom{j}{k}(-\omega)^k \\ &:= \sum_{k=0}^{p-2} \mathrm{C}_k(\alpha)\,\omega^k \quad \text{where } \mathrm{C}_k(\alpha) = (-1)^k \sum_{j=k}^{p-2} a_j \binom{j}{k} \ . \end{aligned} \tag{1}$$

Namely, an algebraic integer $\alpha \in \mathbb{Z}[\zeta]$ can be equally written as $\alpha = \sum_{j=0}^{p-2} c_j\,\omega^j$ with $c_j = \mathrm{C}_j(\alpha) \in \mathbb{Z}$. Note also that writing $\alpha = \sum_{j=0}^{p-2} a_j\,\zeta^j$, we have $\mathrm{C}_0(\alpha) = \sum_{j=0}^{p-2} a_j$ and $\mathrm{C}_1(\alpha) = -\sum_{j=1}^{p-2} a_j\,j$.

The *norm* and *trace* of $\alpha \in \mathbb{Z}[\zeta]$ are the rational integers respectively given by $\mathbf{N}(\alpha) = \prod_{k=1}^{p-1} \sigma_k(\alpha)$ and $\mathbf{T}(\alpha) = \sum_{k=1}^{p-1} \sigma_k(\alpha)$, where $\sigma_k : \zeta \mapsto \zeta^k$. Note that $\mathbf{T}(\alpha) \equiv -\mathrm{C}_0(\alpha) \pmod p$. The *complex conjugate* of α is $\sigma_{-1}(\alpha)$ and is denoted by $\overline{\alpha}$. If $\overline{\alpha} = \alpha$ then α is said to be real.

3 PRIMARY ELEMENTS

We start with the definition as given by Kummer [13, p. 158]. We use the notations of the previous section.

Definition 1. *An element $\alpha \in \mathbb{Z}[\zeta]$ is said to be* primary *whenever it satisfies*

$$\alpha \not\equiv 0 \pmod{\omega}\,, \qquad \alpha \equiv B \pmod{\omega^2}\,, \qquad \alpha\overline{\alpha} \equiv B^2 \pmod p$$

for some $B \in \mathbb{Z}$.

Remark 1. *If only the two first conditions are met, α is said to be* semi-primary.

The next two propositions establish simple criteria for semi-primary and primary elements.

Proposition 1. *Let $\alpha \in \mathbb{Z}[\zeta]$. Then α is semi-primary if $\mathrm{C}_0(\alpha) \not\equiv 0 \pmod p$ and $\mathrm{C}_1(\alpha) \equiv 0 \pmod p$.*

Proof. From Eq. (1), we get $\alpha \equiv \mathrm{C}_0(\alpha) + \mathrm{C}_1(\alpha)\,\omega \pmod{\omega^2}$. Hence, letting $B = \mathrm{C}_0(\alpha) \in \mathbb{Z}$, we have (i) $\alpha \not\equiv 0 \pmod{\omega} \iff \mathrm{C}_0(\alpha) \not\equiv 0 \pmod{\omega}$ and (ii) $\alpha \equiv B \pmod{\omega^2} \iff \mathrm{C}_1(\alpha)\,\omega \equiv 0 \pmod{\omega^2} \iff \mathrm{C}_1(\alpha) \equiv 0 \pmod{\omega}$. As rational integers are congruent modulo ω if and only if they are congruent modulo p, we so obtain the equivalent conditions (i) $\mathrm{C}_0(\alpha) \not\equiv 0 \pmod p$ and (ii) $\mathrm{C}_1(\alpha) \equiv 0 \pmod p$. □

Lemma 1. *If $\alpha \in \mathbb{Z}[\zeta]$, $\alpha \not\equiv \mathrm{C}_0(\alpha) \pmod p$, is real then $\alpha \equiv B + C\,\omega^{2k} \pmod{\omega^{2k+1}}$ for some $B, C \in \mathbb{Z}$, $C \not\equiv 0 \pmod p$, and $1 \leqslant k \leqslant \frac{p-3}{2}$. Moreover, k is uniquely determined by α.*

Proof. Given $\alpha \in \mathbb{Z}[\zeta]$, we can uniquely express α as $\alpha = \mathrm{C}_0(\alpha) + \mathrm{C}_1(\alpha)\,\omega + \cdots + \mathrm{C}_{p-2}(\alpha)\,\omega^{p-2}$. Now, since $\alpha \not\equiv \mathrm{C}_0(\alpha) \pmod p$, there exists an index $1 \leqslant j \leqslant p-2$ with $\mathrm{C}_j(\alpha) \not\equiv 0 \pmod p$—recall that $p \sim \omega^{p-1}$. If we set $m = \arg\min_{1 \leqslant j \leqslant p-2}\big(\mathrm{C}_j(\alpha) \not\equiv 0 \pmod p\big)$, we can write $\alpha \equiv B + C\,\omega^m \pmod{\omega^{m+1}}$ with $B = \mathrm{C}_0(\alpha)$ and $C = \mathrm{C}_m(\alpha)$. Its complex conjugate verifies $\overline{\alpha} \equiv B + C\,\overline{\omega}^m \equiv B + C\,(-\sum_{j=1}^{m} \omega^j)^m \equiv B + C\,(-\omega)^m \pmod{\omega^{m+1}}$. The condition α being real (i.e., $\alpha = \overline{\alpha}$) implies that m is even; say, $m = 2k \in \{1, \ldots, p-2\} \iff 1 \leqslant k \leqslant \frac{p-3}{2}$. □

Proposition 2. *Let $\alpha \in \mathbb{Z}[\zeta]$, α semi-primary. Then α is primary if $\mathrm{C}_{2j}(\alpha\overline{\alpha}) \equiv 0 \pmod p$ for all $1 \leqslant j \leqslant \frac{p-3}{2}$.*

Proof. Define $B = \mathrm{C}_0(\alpha)$ and $\beta = \alpha\overline{\alpha}$. From $\beta \equiv \mathrm{C}_0(\beta) + \mathrm{C}_1(\beta)\,\omega + \cdots + \mathrm{C}_{p-2}(\beta)\,\omega^{p-2} \pmod p$ and since $p \sim \omega^{p-1}$, we have $\mathrm{C}_0(\beta) \equiv \mathrm{C}_0(\alpha)^2 \equiv B^2 \pmod{\omega} \iff \mathrm{C}_0(\beta) \equiv B^2 \pmod p$. Consequently, the third condition in Definition 1 becomes $\mathrm{C}_j(\beta) \equiv 0 \pmod{\omega} \iff \mathrm{C}_j(\beta) \equiv 0 \pmod p$, for all $1 \leqslant j \leqslant p-2$.

If $\beta \equiv \mathrm{C}_0(\beta) \pmod p$ then $\beta \equiv B^2 \pmod p$ and thus α is primary. We henceforth assume that $\beta \not\equiv \mathrm{C}_0(\beta) \pmod p)$. Noticing that $\beta = \alpha\overline{\alpha}$ is real, we can apply Lemma 1. We obtain $\beta \equiv B^2 + C\,\omega^{2k} \pmod{\omega^{2k+1}}$ for some $1 \leqslant k \leqslant \frac{p-3}{2}$ and where $C \equiv \mathrm{C}_{2k}(\beta) \pmod p$. In particular, this implies $\mathrm{C}_1(\beta) \equiv 0 \pmod p$. Furthermore, by assumption, $\mathrm{C}_{2j}(\beta) \equiv 0 \pmod p$ for all $1 \leqslant j \leqslant \frac{p-3}{2}$. It remains to show that $\mathrm{C}_{2j+1}(\beta) \equiv 0 \pmod p$ for all $1 \leqslant j \leqslant \frac{p-3}{2}$. This follows by successive applications of Lemma 1: $\mathrm{C}_1(\beta) \equiv 0 \pmod p$ and $\mathrm{C}_2(\beta) \equiv 0 \pmod p$ imply $C_3(\beta) \equiv 0 \pmod p$; in turn, together with $\mathrm{C}_4(\beta) \equiv 0 \pmod p$ imply $\mathrm{C}_5(\beta) \equiv 0 \pmod p$; and so on... until $\mathrm{C}_{p-2}(\beta) \equiv 0 \pmod p$. □

4 OBTAINING PRIMARY ASSOCIATES

As a consequence of Dirichlet's unit theorem, the group of units of $\mathbb{Z}[\zeta]$ is the direct product of $\langle \pm\zeta\rangle$ and a free abelian group $\mathcal{E}$ of rank $r = \frac{p-3}{2}$. The generators of $\mathcal{E}$ are called *fundamental units* and will be denoted by $\eta_1, \dots, \eta_r$.

The next proposition states that among the associates of an algebraic integer, we may distinguish one (up to the sign) which is primary. Clearly, from Definition 1, if α^* is primary then $-\alpha^*$ is also primary.

Proposition 3. *Every element $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$ has a primary associate α^* of the form*

$$\alpha^* = \pm\,\zeta^{e_0}\,{\eta_1}^{e_1}\cdots{\eta_r}^{e_r}\,\alpha \quad \text{where } 0 \leqslant e_0, e_1, \dots, e_r \leqslant p-1 \ .$$

Moreover, α^* is unique up to its sign.

Proof. See [4, Lemma 2.6]. □

The following lemma is useful.

Lemma 2. *If $\alpha, \alpha' \in \mathbb{Z}[\zeta]$ are semi-primary then so is $\alpha\alpha'$.*

Proof. Let $\alpha, \alpha' \in \mathbb{Z}[\zeta]$ with $\mathrm{C}_0(\alpha), \mathrm{C}_0(\alpha') \not\equiv 0 \pmod{p}$ and $\mathrm{C}_1(\alpha) \equiv \mathrm{C}_1(\alpha') \equiv 0 \pmod{p}$. Write $\alpha = \sum_{j=0}^{p-2} a_j\,\zeta^j$. It is worth seeing that $\alpha^p \equiv (a_0 + a_1\,\zeta + \cdots + a_{p-2}\,\zeta^{p-2})^p \equiv \sum_{j=0}^{p-2} a_j \equiv \mathrm{C}_0(\alpha) \pmod{p}$, and similarly for α'. Hence, we obtain $\mathrm{C}_0(\alpha\alpha') \equiv (\alpha\alpha')^p \equiv \alpha^p\,\alpha'^p \equiv \mathrm{C}_0(\alpha)\,\mathrm{C}_0(\alpha') \pmod{p}$.

Moreover, from $\alpha\,\omega = \sum_{k=0}^{p-2} \mathrm{C}_k(\alpha)\,\omega^{k+1} \equiv \sum_{k=1}^{p-2} \mathrm{C}_{k-1}(\alpha)\,\omega^k + \mathrm{C}_{p-2}(\alpha)\,\omega^{p-1} \equiv \sum_{k=1}^{p-2} \mathrm{C}_{k-1}(\alpha)\,\omega^k \pmod{p}$ and $\alpha\,\omega = \sum_{k=0}^{p-2} \mathrm{C}_k(\alpha\,\omega)\,\omega^k \equiv \sum_{k=1}^{p-2} \mathrm{C}_k(\alpha\,\omega)\,\omega^k \pmod{p}$ since $\mathrm{C}_0(\omega) = 0$, it follows that $\mathrm{C}_k(\alpha\,\omega) \equiv \mathrm{C}_{k-1}(\alpha) \pmod{p}$, for $1 \leqslant k \leqslant p-2$. In particular, we have $\mathrm{C}_1(\alpha\,\omega) \equiv \mathrm{C}_0(\alpha) \pmod{p}$. Letting $\alpha' = \sum_{j=0}^{p-2} c'_j\,\omega^j$ with $c'_j = \mathrm{C}_j(\alpha')$, we so get $\mathrm{C}_1(\alpha\alpha') = \mathrm{C}_1(\alpha\sum_{j=0}^{p-2} c'_j\,\omega^j) = \sum_{j=0}^{p-2} c'_j\,\mathrm{C}_1(\alpha\,\omega^j) \equiv c'_0\,\mathrm{C}_1(\alpha) + \sum_{j=1}^{p-2} c'_j\,\mathrm{C}_0(\alpha\,\omega^{j-1}) \equiv c'_0\,\mathrm{C}_1(\alpha) + c'_1\,\mathrm{C}_0(\alpha) + \sum_{j=2}^{p-2} c'_j\,\mathrm{C}_0(\alpha)\,\mathrm{C}_0(\omega)^{j-1} \equiv \mathrm{C}_0(\alpha')\,C_1(\alpha) + \mathrm{C}_1(\alpha')\,\mathrm{C}_0(\alpha) \pmod{p}$.

As a result, from $\mathrm{C}_0(\alpha\alpha') \equiv \mathrm{C}_0(\alpha)\,\mathrm{C}_0(\alpha') \pmod{p}$ and $\mathrm{C}_1(\alpha\alpha') \equiv \mathrm{C}_0(\alpha)\,\mathrm{C}_1(\alpha') + \mathrm{C}_0(\alpha')\,\mathrm{C}_1(\alpha) \pmod{p}$, we get $\mathrm{C}_0(\alpha\alpha') \not\equiv 0 \pmod{p}$ and $\mathrm{C}_1(\alpha\alpha') \equiv 0 \pmod{p}$; that is, $\alpha\alpha'$ is semi-primary. □

Theorem 1. *Let $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$. Then $\alpha\,\zeta^s$ with $s = \frac{\mathrm{C}_1(\alpha)}{\mathrm{C}_0(\alpha)} \bmod p$ is semi-primary.*

Proof. Note that the condition $\alpha \not\equiv 0 \pmod{\omega}$ is equivalent to $\mathrm{C}_0(\alpha) \not\equiv 0 \pmod{p}$. Let $\alpha^{[1]} = \alpha\,\zeta^s$ with $s = \frac{\mathrm{C}_1(\alpha)}{\mathrm{C}_0(\alpha)} \bmod p$. We need to check the conditions of Proposition 1. In the proof of Lemma 2, we showed that, for every $\alpha, \alpha' \in \mathbb{Z}[\zeta]$, $\mathrm{C}_0(\alpha\alpha') \equiv \mathrm{C}_0(\alpha)\,\mathrm{C}_0(\alpha') \pmod{p}$ and $\mathrm{C}_1(\alpha\alpha') \equiv \mathrm{C}_0(\alpha)\,\mathrm{C}_1(\alpha') + \mathrm{C}_0(\alpha')\,\mathrm{C}_1(\alpha) \pmod{p}$. By induction, we therefore get $\mathrm{C}_0(\zeta^s) \equiv \mathrm{C}_0(\zeta)^s \equiv 1 \pmod{p}$ and $\mathrm{C}_1(\zeta^s) \equiv s\mathrm{C}_1(\zeta) \equiv -s \pmod{p}$. So, we have $\mathrm{C}_0(\alpha^{[1]}) \equiv \mathrm{C}_0(\alpha\,\zeta^s) \equiv \mathrm{C}_0(\alpha)\,\mathrm{C}_0(\zeta^s) \equiv \mathrm{C}_0(\alpha) \pmod{p}$ and thus $\mathrm{C}_0(\alpha^{[1]}) \not\equiv 0 \pmod{p}$. We also have $\mathrm{C}_1(\alpha^{[1]}) \equiv \mathrm{C}_1(\alpha\,\zeta^s) \equiv \mathrm{C}_0(\alpha)\,\mathrm{C}_1(\zeta^s) + \mathrm{C}_0(\zeta)^s\,\mathrm{C}_1(\alpha) \equiv -s\mathrm{C}_0(\alpha) + \mathrm{C}_1(\alpha) \equiv 0 \pmod{p}$ since $s = \frac{\mathrm{C}_1(\alpha)}{\mathrm{C}_0(\alpha)} \bmod p$. □

Theorem 1 provides an efficient way to produce a semi-primary associate. Now, suppose we are given two semi-primary integers $\alpha, \varepsilon_k \in \mathbb{Z}[\zeta]$. Lemma 2 teaches that $\alpha\,\varepsilon_k$ is also semi-primary. The same holds true by induction for $\alpha \leftarrow \alpha\,{\varepsilon_k}^{e_k}$, for any exponent $e_k \geqslant 1$.

Suppose further that the resulting α satisfies

$$\mathrm{C}_{2j}(\alpha\overline{\alpha}) \equiv 0 \pmod{p} \quad \text{for all } 1 \leqslant j \leqslant k \ . \tag{2}$$

As will become apparent (cf. Theorem 2), by Proposition 2, iterating this process for $k = 1, \dots, \frac{p-3}{2}$ eventually yields a primary element. Moreover, if all involved ε_k are units then the so-obtained primary element is also an associate. In order to make the above process work, the updating step (i.e., $\alpha \leftarrow \alpha\,{\varepsilon_k}^{e_k}$) should be such that Equation (2) remains fulfilled for the new α when k is incremented. This can achieved by selecting real units ε_k of the form

$$\varepsilon_k \equiv E_k + F_k\,\omega^{2k} \pmod{\omega^{2k+1}} \quad \text{with } E_k, F_k \in \mathbb{Z} \text{ and } E_k, F_k \not\equiv 0 \pmod{p}\ , \tag{3}$$

for $1 \leqslant k \leqslant \frac{p-3}{2}$; cf. Lemma 1. Note that as defined by Eq. (3), units ε_k are semi-primary.

Theorem 2. *Given some integer $k \geqslant 1$, let $\alpha \in \mathbb{Z}[\zeta]$, α semi-primary, such that $\mathrm{C}_{2j}(\alpha\overline{\alpha}) \equiv 0 \pmod{p}$ for all $1 \leqslant j \leqslant k-1$ and a real unit $\varepsilon \in \mathbb{Z}[\zeta]$ such that $\varepsilon \equiv \mathrm{C}_0(\varepsilon) + \mathrm{C}_{2k}(\varepsilon)\,\omega^{2k} \pmod{\omega^{2k+1}}$ with $\mathrm{C}_0(\varepsilon), \mathrm{C}_{2k}(\varepsilon) \not\equiv 0 \pmod{p}$. Then $\alpha' := \alpha\,\varepsilon^t$ with $t = -\frac{\mathrm{C}_{2k}(\alpha\overline{\alpha})\,\mathrm{C}_0(\varepsilon)}{2\mathrm{C}_0(\alpha\overline{\alpha})\,\mathrm{C}_{2k}(\varepsilon)} \bmod p$ is semi-primary and $\mathrm{C}_{2j}(\alpha'\,\overline{\alpha'}) \equiv 0 \pmod{p}$ for all $1 \leqslant j \leqslant k$.*

Proof. Since ε is semi-primary, $\alpha' = \alpha\varepsilon^t$ is semi-primary for any t by Lemma 2. Further, since ε is real (i.e., $\varepsilon = \overline{\varepsilon}$), it follows that $\alpha'\overline{\alpha'} = \alpha\overline{\alpha}\varepsilon^{2t}$. From Lemma 1, as $\alpha\overline{\alpha}$ is real and since $\mathrm{C}_{2j}(\alpha\overline{\alpha}) \equiv 0 \pmod p$ for all $1 \leqslant j \leqslant k-1$, we deduce that $\alpha\overline{\alpha} \equiv \mathrm{C}_0(\alpha\overline{\alpha}) + \mathrm{C}_{2k}(\alpha\overline{\alpha})\,\omega^{2k} \pmod{\omega^{2k+1}}$. Hence, we get $\alpha'\overline{\alpha'} \equiv \big(\mathrm{C}_0(\alpha\overline{\alpha}) + \mathrm{C}_{2k}(\alpha\overline{\alpha})\,\omega^{2k}\big)\big(\mathrm{C}_0(\varepsilon) + \mathrm{C}_{2k}(\varepsilon)\,\omega^{2k}\big)^{2t} \equiv \big(\mathrm{C}_0(\alpha\overline{\alpha}) + \mathrm{C}_{2k}(\alpha\overline{\alpha})\,\omega^{2k}\big)\big(\mathrm{C}_0(\varepsilon)^{2t} + 2t\,\mathrm{C}_0(\varepsilon)^{2t-1}\,\mathrm{C}_{2k}(\varepsilon)\,\omega^{2k}\big) \pmod{\omega^{2k+1}}$ and thus $\mathrm{C}_{2k}(\alpha'\overline{\alpha'}) \equiv 2t\,\mathrm{C}_0(\alpha\overline{\alpha})\,\mathrm{C}_0(\varepsilon)^{2t-1}\,\mathrm{C}_{2k}(\varepsilon) + \mathrm{C}_{2k}(\alpha\overline{\alpha})\,\mathrm{C}_0(\varepsilon)^{2t} \pmod p$. Consequently, since $\mathrm{C}_0(\varepsilon) \not\equiv 0 \pmod p$, we so have $\mathrm{C}_{2k}(\alpha'\overline{\alpha'}) \equiv 0 \pmod p \iff 2t\,\mathrm{C}_0(\alpha\overline{\alpha})\,\mathrm{C}_{2k}(\varepsilon) + \mathrm{C}_{2k}(\alpha\overline{\alpha})\,\mathrm{C}_0(\varepsilon) \equiv 0 \pmod p \iff t \equiv -\frac{\mathrm{C}_{2k}(\alpha\overline{\alpha})\,\mathrm{C}_0(\varepsilon)}{2\mathrm{C}_0(\alpha\overline{\alpha})\,\mathrm{C}_{2k}(\varepsilon)} \pmod p$ since $\mathrm{C}_0(\alpha\overline{\alpha}) \not\equiv 0 \pmod p$ ($\alpha\overline{\alpha}$ being semi-primary from Lemma 2) and $\mathrm{C}_{2k}(\varepsilon) \not\equiv 0 \pmod p$ by assumption. ◻

The existence of a set of fundamental real units $\{\varepsilon_1, \dots, \varepsilon_r\}$ with $r = \frac{p-3}{2}$ of the form (3) is a result of Dénes [9]; see also [20, pp. 192–193] and [23, Theorem 2]. Let $\varepsilon^+ = (\zeta^{g/2} - \zeta^{-g/2})/(\zeta^{\frac12} - \zeta^{-\frac12})$ where g is an odd primitive root modulo p. Then the units ε_k, $1 \leqslant k \leqslant r$, given by

$$\begin{aligned}\varepsilon_k &= (\varepsilon^+)^{\sum_{j=0}^{p-2} \sigma_g{}^j\, g^{-2jk} \bmod p} \qquad \text{where } \sigma_g\colon \zeta \mapsto \zeta^g\\ &= \prod_{j=0}^{p-2}\left(\frac{\zeta^{\frac{g^{j+1}}{2}} - \zeta^{-\frac{g^{j+1}}{2}}}{\zeta^{\frac{g^j}{2}} - \zeta^{-\frac{g^j}{2}}}\right)^{g^{-2jk} \bmod p}\end{aligned} \tag{4}$$

are real and satisfy Equation (3) with $E_k \equiv \mathrm{C}_0(\varepsilon_k) \pmod p$ and $F_k \equiv \mathrm{C}_{2k}(\varepsilon_k) \pmod p$.

We now have all the ingredients to obtain a primary element α^* as per Proposition 3. Starting with $\alpha^{[0]} \leftarrow \alpha$ and iterating as

$$\begin{cases}\alpha^{[1]} \leftarrow \alpha^{[0]}\,\zeta^{e_0} \ \text{ with } e_0 = \frac{\mathrm{C}_1(\alpha^{[0]})}{\mathrm{C}_0(\alpha^{[0]})} \bmod p \quad \text{(Theorem 1)}\\ \alpha^{[k+1]} \leftarrow \alpha^{[k]}\,\varepsilon_k{}^{e_k} \ \text{ with } e_k = -\frac{\mathrm{C}_{2k}(\beta^{[k]})\,\mathrm{C}_0(\varepsilon)}{2\mathrm{C}_0(\beta^{[k]})\,\mathrm{C}_{2k}(\varepsilon)} \bmod p \quad \text{(Theorem 2)}, \quad \text{for } 1 \leqslant k \leqslant r\end{cases}$$

where $\beta^{[k]} = \alpha^{[k]}\overline{\alpha^{[k]}}$ and $r = \frac{p-3}{2}$, we obtain $\alpha^{[r+1]} \leftarrow \alpha^{[0]}\,\zeta^{e_0}\,\varepsilon_1{}^{e_1}\cdots\varepsilon_r{}^{e_r}$, which is primary. Knowing that two primary associates only differ by a p^{th}-power unit, exponents e_j ($0 \leqslant j \leqslant r$) can be reduced modulo p. Finally, if the resulting primary associate has to be expressed with respect to a given set of fundamental units $\{\eta_1, \dots, \eta_r\}$, from the decompositions $\varepsilon_j = \zeta^{f_{j,0}}\prod_{k=1}^r \eta_k{}^{f_{j,k}}$ with $f_{j,k} \in \mathbb{Z}$, we write $\alpha^{[r+1]} \leftarrow \alpha^{[0]}\,\zeta^{e_0}\prod_{j=1}^r \varepsilon_j{}^{e_j} = \alpha^{[0]}\,\zeta^{e_0}\prod_{j=1}^r(\zeta^{e_j f_{j,0}}\prod_{k=1}^r \eta_k{}^{e_j f_{j,k}}) = \alpha^{[0]}\,\zeta^{e_0'}\prod_{k=1}^r \eta_k{}^{e_k'}$ where $e_0' = e_0 + \sum_{j=1}^r e_j f_{j,0}$ and $e_k' = \sum_{j=1}^r e_j f_{j,k}$, for $1 \leqslant k \leqslant r$, or using matrix notation,

$$(e_0', \dots, e_r') = \mathcal{T}(e_0, \dots, e_r) \quad \text{with } \mathcal{T}(e_0, \dots, e_r) = \left[\begin{pmatrix} 1 & f_{1,0} & \cdots & f_{r,0}\\ 0 & f_{1,1} & \cdots & f_{r,1}\\ \vdots & \vdots & & \vdots\\ 0 & f_{1,r} & \cdots & f_{r,r}\end{pmatrix}\begin{pmatrix} e_0\\ e_1\\ \vdots\\ e_r\end{pmatrix}\right]^{\mathsf{T}}.$$

We define

$$\alpha^* = \alpha^{[0]}\,\zeta^{e_0' \bmod p}\,\eta_1{}^{e_1' \bmod p}\cdots\eta_r{}^{e_r' \bmod p}.$$

Putting it all together, this yields a generic algorithm for finding primary associates along with their representation; see Algorithm 1. On input $\alpha \in \mathbb{Z}[\zeta]$ with $\mathbf{T}(\alpha) \not\equiv 0 \pmod p$, the algorithm outputs the primary associate α^* with respect to basis $\{\eta_1, \dots, \eta_r\}$ and the representation vector $(e_0, e_1, \dots, e_r)$, such that $\alpha^* = \zeta^{e_0}\eta_1{}^{e_1}\cdots\eta_r{}^{e_r}\,\alpha$. We write `primary`$(\alpha) \leftarrow \alpha^*$ and `repr`$(\alpha) \leftarrow (e_0, e_1, \dots, e_r)$. The algorithm internally makes use of the set of real units $\{\varepsilon_1, \dots, \varepsilon_r\}$ as defined in Eq. (4) and corresponding conversion transform $\mathcal{T}$.

5 COMPUTING SYMBOLS

If $\mathbb{Z}[\zeta]$ is norm-Euclidean, there exists for all pairs $\alpha, \beta \in \mathbb{Z}[\zeta]$ with $\beta \neq 0$ an element $\rho \in \mathbb{Z}[\zeta]$ such that $\alpha \equiv \rho \pmod \beta$ and $\mathbf{N}(\rho) < \mathbf{N}(\beta)$. Explicit algorithms for finding ρ are known; see [16] for $p \leqslant 11$ and [17] for $p = 13$. We refer to such an algorithm as `euclid_div()`. The Caranay–Scheidler algorithm [4] (initially given in the context of $p = 7$) can then be extended to compute higher-order power residue symbols. Recall that $\omega = 1 - \zeta$. For $\alpha, \pi \in \mathbb{Z}[\zeta]$ with π a prime such that $\pi \nsim \omega$ and $\pi \nmid \alpha$, the p^{th} *power residue symbol* $\left[\frac{\alpha}{\pi}\right]_p$ is defined to be the p^{th} root of unity ζ^i such that

$$\alpha^{(\mathbf{N}(\pi)-1)/p} \equiv \zeta^i \pmod \pi$$

and the integer i is called the *index* of α with respect to π, henceforth denoted $\mathrm{ind}_\pi(\alpha)$. In a way similar to the Legendre symbol, the definition generalizes: If $\lambda \in \mathbb{Z}[\zeta]$ is non-unit and $\gcd(\lambda, \omega) \sim 1$ then, writing $\lambda = \prod_j \pi_j{}^{e_j}$

Algorithm 1: Computing $\alpha^* \sim \alpha$ and its representation

Input: $\alpha \in \mathbb{Z}[\zeta]$ with $\mathbf{T}(\alpha) \not\equiv 0 \pmod{p}$
Output: $\alpha^* \leftarrow \texttt{primary}(\alpha)$ and $(e_0, e_1, \ldots, e_r) \leftarrow \texttt{repr}(\alpha)$ with $\alpha^* = \zeta^{e_0} {\eta_1}^{e_1} \cdots {\eta_r}^{e_r} \alpha$ and $r = \frac{p-3}{2}$

$e_0 \leftarrow \mathrm{C}_1(\alpha)/\mathrm{C}_0(\alpha) \bmod p$
$\alpha \leftarrow \zeta^{e_0} \alpha$; $\beta \leftarrow \alpha\overline{\alpha}$
for $k = 1$ **to** $\frac{p-3}{2}$ **do**
  $e_k \leftarrow -\dfrac{\mathrm{C}_{2k}(\beta)\,\mathrm{C}_0(\varepsilon_k)}{2\mathrm{C}_0(\beta)\,\mathrm{C}_{2k}(\varepsilon_k)} \bmod p$
  $\beta \leftarrow \beta {\varepsilon_k}^{2e_k}$
end
$(e_0, e_1, \ldots, e_r) \leftarrow \tau(e_0, e_1, \ldots, e_r) \bmod p$
$\alpha^* \leftarrow \zeta^{e_0} {\eta_1}^{e_1} \cdots {\eta_r}^{e_r} \alpha$
return $[\alpha^*, (e_0, e_1, \ldots, e_r)]$

for primes π_j in $\mathbb{Z}[\zeta]$, the (generalized) p^{th} power residue symbol $\left[\frac{\alpha}{\lambda}\right]_p$ is defined as $\left[\frac{\alpha}{\lambda}\right]_p = \prod_j \left[\frac{\alpha}{\pi_j}\right]_p^{e_j}$. Provided that p is a regular prime (which is verified for all odd primes $p \leqslant 13$), *Kummer's reciprocity law* [13] states that for any two primary elements $\alpha, \lambda \in \mathbb{Z}[\zeta]$,

$$\left[\frac{\alpha}{\lambda}\right]_p = \left[\frac{\lambda}{\alpha}\right]_p \;.$$

This leads to Algorithm 2 given below (where for compactness we have set $\eta_0 = \zeta$).

Algorithm 2: Computing the p^{th} power residue symbol

Input: $\alpha, \lambda \in \mathbb{Z}[\zeta]$ with $\gcd(\alpha, \lambda) \sim 1$ and $\mathbf{T}(\lambda) \not\equiv 0 \pmod{p}$
Output: $\left[\frac{\alpha}{\lambda}\right]_p$

$\lambda^* \leftarrow \texttt{primary}(\lambda)$
$j \leftarrow 0$
while $\mathbf{N}(\lambda^*) > 1$ **do**
  $\rho \leftarrow \texttt{euclid\_div}(\alpha, \lambda^*)$
  $s \leftarrow 0$
  while $\mathbf{T}(\rho) \equiv 0 \pmod{p}$ **do**
    $s \leftarrow s + 1$
    $\rho \leftarrow \rho \div \omega$
  end
  $[\rho^*, (e_0, \ldots, e_r)] \leftarrow [\texttt{primary}(\rho), \texttt{repr}(\rho)]$ // $\rho^* = \zeta^{e_0} {\eta_1}^{e_1} \cdots {\eta_r}^{e_r} \rho$
  $j \leftarrow j + s \cdot \mathrm{ind}_{\lambda^*}(\omega)$
  for $i = 0$ **to** r **do**
    $j \leftarrow j - e_i \cdot \mathrm{ind}_{\lambda^*}(\eta_i)$
  end
  $\alpha \leftarrow \lambda^*$; $\lambda^* \leftarrow \rho^*$
end
return ζ^j

6 NINTH- AND SIXTEENTH-POWER RESIDUE SYMBOLS

In this section, we study the 9^{th}- and the 16^{th} power residue symbols.

9^{th} power residue symbol For $p = 9$, the ring $\mathbb{Z}[\zeta_9]$ is known to be norm-Euclidean [5]; see [6, § 3] for a division algorithm. The previous framework does not readily apply to this case; we nevertheless still obtain a reciprocity law and complementary laws through decomposition. Let $\zeta := \zeta_9$ and $\omega = 1 - \zeta$. For $\alpha, \beta \in \mathbb{Z}[\zeta]$ co-prime with ω, we can write

$$\alpha = \prod_{i=1}^{15} (1+\omega^i)^{e_i} \mod \omega^{15} , \qquad \beta = \prod_{i=1}^{15} (1+\omega^i)^{f_i} \mod \omega^{15}$$

with integer exponents e_i, f_i and $e_1, f_1 \in \{0,1\}$. There are 4×15 integer constants $U_{j,i}$ so that

$$k_j = \sum_{i=1}^{15} U_{j,i}\, e_i$$

makes the following "complementary laws" hold:

$$\left[\frac{\zeta}{\alpha}\right]_9 = z^{k_1} , \qquad \left[\frac{1+\zeta}{\alpha}\right]_9 = z^{k_2} , \qquad \left[\frac{1+\zeta^2}{\alpha}\right]_9 = z^{k_3} , \qquad \left[\frac{\omega}{\alpha}\right]_9 = z^{k_4} .$$

Importantly, the constants $U_{j,i}$ do not depend on α. Similarly there is a fixed 15×15 matrix $(T_{i,j})$ with integer coefficients so that we have this ninth reciprocity law:

$$\left[\frac{\alpha}{\beta}\right]_9 = \left[\frac{\beta}{\alpha}\right]_9 \cdot z^k \qquad \text{where } k = \sum_{i,j} T_{i,j}\, e_i\, f_j \ .$$

The matrices are given below:

$$T = \begin{pmatrix}
0 & 5 & 3 & 7 & 1 & 8 & 7 & 5 & 3 & 6 & 3 & 3 & 6 & 3 & 0 \\
4 & 0 & 4 & 3 & 2 & 3 & 1 & 6 & 6 & 3 & 3 & 0 & 6 & 0 & 0 \\
6 & 5 & 0 & 6 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 6 & 3 & 0 & 5 & 0 & 6 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\
8 & 7 & 0 & 4 & 0 & 0 & 3 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\
1 & 6 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 8 & 0 & 3 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 3 & 0 & 3 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
3 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 6 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\qquad
U = \begin{pmatrix}
8 & 6 & 1 & 0 \\
4 & 6 & 7 & 0 \\
8 & 6 & 1 & 0 \\
5 & 4 & 3 & 0 \\
1 & 7 & 7 & 0 \\
7 & 8 & 7 & 6 \\
7 & 4 & 6 & 0 \\
1 & 2 & 7 & 0 \\
0 & 3 & 3 & 8 \\
0 & 6 & 3 & 0 \\
0 & 3 & 0 & 0 \\
6 & 3 & 6 & 6 \\
6 & 6 & 0 & 0 \\
6 & 3 & 6 & 0 \\
0 & 0 & 0 & 3
\end{pmatrix}$$

A complete algorithm for computing the 9th power residue symbol using these matrices is given in Appendix A.

16th power residue symbol The same can be done very similarly in the norm-Euclidean ring $\mathbb{Z}[\zeta_{16}]$ (see [19] for a proof of the division property and [6, § 5] for a division algorithm) with $\zeta := \zeta_{16}$ a 16th root of unity and $\omega = 1 - \zeta$. Then, for $\alpha, \beta \in \mathbb{Z}[\zeta]$ co-prime with 2, we can write:

$$\alpha = \prod_{i=1}^{40} (1+\omega^i)^{e_i} \mod \omega^{41} , \qquad \beta = \prod_{i=1}^{40} (1+\omega^i)^{f_i} \mod \omega^{41}$$

with integer exponents e_i, f_i and $e_1, f_1 \in \{0,1\}$. There are 5×40 integer constants $U_{j,i}$ so that

$$k_j = \sum_{i=1}^{40} U_{j,i}\, e_i$$

makes the following equalities hold:

$$\left[\frac{\zeta}{\alpha}\right]_{16} = z^{k_1} , \quad \left[\frac{1+\zeta+\zeta^2}{\alpha}\right]_{16} = z^{k_2} , \quad \left[\frac{1+\zeta^2+\zeta^4}{\alpha}\right]_{16} = z^{k_3} , \quad \left[\frac{1+\zeta^3+\zeta^6}{\alpha}\right]_{16} = z^{k_4} , \quad \left[\frac{\omega}{\alpha}\right]_{16} = z^{k_5} .$$

Again, the constants $U_{j,i}$ do not depend on α. Similarly there is a fixed 40×40 matrix $(T_{i,j})$ with integer coefficients so that we have this sixteenth reciprocity law:

$$\left[\frac{\alpha}{\beta}\right]_{16} = \left[\frac{\beta}{\alpha}\right]_{16} \cdot z^k \qquad \text{where } k = \sum_{i,j} T_{i,j}\, e_i\, f_j \ .$$

The matrices T and U are given below:

$$T = \begin{pmatrix}
0&2&5&13&4&10&5&15&15&7&7&9&15&13&15&10&14&2&6&14&2&6&10&0&0&8&8&12&4&4&12&8&8&8&8&8&8&8&8 \\
14&0&14&2&15&2&5&14&2&14&6&10&8&14&4&4&8&12&8&12&0&4&0&0&0&0&0&8&0&8&0&0&0&0&0&0&0&0&0 \\
11&2&0&3&14&14&9&12&14&13&0&2&15&8&14&4&0&10&12&12&6&12&4&8&4&4&8&8&12&0&8&0&0&8&0&0&8&0&0 \\
3&14&13&8&2&2&4&4&8&12&8&12&8&8&0&8&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
12&1&2&14&8&3&12&4&14&12&13&4&12&14&4&8&12&12&2&0&8&12&4&0&0&0&4&0&0&8&0&0&0&0&8&0&0&0&0 \\
6&14&2&14&13&0&8&0&10&14&4&4&4&0&0&8&8&12&0&8&0&8&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
11&11&7&12&4&8&0&8&15&10&12&0&12&4&8&8&6&4&0&0&12&0&8&0&12&8&0&0&0&0&0&0&8&0&0&0&0&0&0 \\
1&2&4&12&12&0&8&8&8&8&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
1&14&2&8&2&6&1&8&8&12&4&8&0&12&10&0&8&0&4&0&8&8&4&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0 \\
9&2&3&4&4&2&6&8&4&8&12&8&0&4&8&0&0&8&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
9&10&0&8&3&12&4&8&12&4&8&0&14&0&8&0&12&8&8&0&12&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0 \\
7&6&14&4&12&12&0&0&8&8&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
1&8&1&8&4&12&4&0&0&0&2&0&8&8&4&0&8&0&4&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0 \\
3&2&8&8&2&0&12&0&4&12&0&0&8&8&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
1&12&2&0&12&0&8&0&6&8&8&0&12&0&8&0&12&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
6&12&12&8&8&8&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
2&8&0&0&4&8&10&0&8&0&4&0&8&0&4&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
14&4&6&0&4&4&12&0&0&8&8&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
10&8&4&0&14&0&0&0&12&0&8&0&12&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
2&4&4&8&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
14&0&10&0&8&0&4&0&8&0&4&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
10&12&4&0&4&8&0&0&8&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
6&0&12&0&12&0&8&0&12&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
0&0&12&0&0&0&4&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
8&0&12&0&0&8&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
8&0&8&0&12&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
4&8&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
12&0&4&0&0&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
12&8&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
4&0&8&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
8&0&0&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
8&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
8&0&0&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
8&0&8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
8&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

$$U^{\intercal} = \begin{pmatrix}
0&2&0&5&7&10&2&7&15&7&3&1&1&13&13&10&10&2&2&14&14&6&6&0&0&8&8&12&12&4&4&8&8&8&8&8&8&8&8&0&0 \\
7&8&7&10&11&2&14&5&13&10&15&9&14&7&3&10&10&8&2&14&8&14&10&8&12&12&8&12&0&12&12&8&8&0&8&8&0&8&8&0&0 \\
2&8&2&0&5&6&2&2&12&0&8&2&14&2&2&4&12&0&8&12&12&4&4&0&0&8&8&8&8&8&8&0&0&0&0&0&0&0&0&0&0 \\
4&1&4&2&6&6&0&3&12&4&1&15&4&13&9&14&12&4&6&2&8&2&6&8&8&12&8&4&8&4&4&8&0&0&8&8&0&8&8&0&0 \\
0&0&0&10&8&0&0&5&8&4&8&6&8&12&8&13&0&8&0&12&0&8&0&10&0&8&0&4&0&8&0&4&0&0&0&0&0&0&0&8&0
\end{pmatrix}$$

7 CONCLUSION AND FURTHER RESEARCH

The methods described in this paper enable the computation of p^{th} power residue symbols up to and including $p = 13$ when p is prime. Whether for $p = 17$ and $p = 19$ there is an Euclidean division seems (to the best of our understanding) currently unknown and perhaps an alternative strategy must be found. The problem gets harder beyond $p = 23$, as the ideal class group is no longer trivial, and in particular is difficult for $p = 37$ which is not a regular prime (and therefore Kummer's theory does not apply).

We also provide algorithms for the 9^{th} and 16^{th} power residue symbols, which may be extended albeit may require a more compact formulation.

REFERENCES

[1] William D. Banks, Daniel Lieman, and Igor E. Shparlinski. "An extremely small and efficient identification scheme". In: *Information Security and Privacy (ACISP 2000)*. Ed. by E. Dawson et al. Vol. 1841. Lecture Notes in Computer Science. Springer, 2000, pp. 378–384. DOI: 10.1007/10718964_31.

[2] Éric Brier, Houda Ferradi, Marc Joye, and David Naccache. "New number-theoretic cryptographic primitives". In: *Journal of Mathematical Cryptology* 14.1 (2020), pp. 1831–1853. DOI: 10.1515/jmc-2019-0035.

[3] Éric Brier and David Naccache. *The thirteenth power residue symbol*. Cryptology ePrint Archive, Report 2019/1176. 2019. URL: https://ia.cr/2019/1176.

[4] Perlas C. Caranay and Renate Scheidler. "An efficient seventh power residue symbol algorithm". In: *International Journal of Number Theory* 6.8 (2010), pp. 1831–1853. DOI: 10.1142/s1793042110003770.

[5] Augustin-Louis Cauchy. "Mémoire sur de nouvelles formules relatives à la théorie des polynômes radicaux, et sur le dernier théorème de Fermat". In: *Comptes Rendus des Séances de l'Académie des Sciences de Paris* 24 (1847), pp. 516–528.

[6] Tito Chella. "Dimostrazione dell'esistenza di un algoritmo delle divisioni successive per alcuni corpi circolari". In: *Annali di Matematica Pura ed Applicata* 1.1 (1927), pp. 199–218. DOI: 10.1007/BF02409920.

[7] Ivan Bjerre Damgård and Gudmund Skovbjerg Frandsen. "Efficient algorithms for the gcd and cubic residuosity in the ring of Eisenstein integers". In: *Journal of Symbolic Computation* 39.6 (2005), pp. 643–652. DOI: 10.1016/j.jsc.2004.02.006.

[8] Koen de Boer and Carlo Pagano. "Calculating the power residue symbol and ibeta: Applications of computing the group structure of the principal units of a $\mathfrak{p}$-adic number field completion". In: *42nd International Symposium on Symbolic and Algebraic Computation*. Ed. by M. A. Burr et al. ACM, 2017, pp. 117–124. DOI: 10.1145/3087604.3087637.

[9] Péter Dénes. "Über Grundeinheitssysteme der irregulären Kreiskörper van besonderen Kongruenzeigenschaften". In: *Publ. Math. Debrecen* 3 (1954), pp. 195–204.

[10] Shafi Goldwasser and Silvio Micali. "Probabilistic encryption". In: *Journal of Computer and System Sciences* 28.2 (1984), pp. 270–299. DOI: 10.1016/0022-0000(84)90070-9.

[11] Marc Joye. *Evaluating octic residue symbols*. Cryptology ePrint Archive, Report 2019/1196. 2019. URL: https://ia.cr/2019/1196.

[12] Marc Joye, Oleksandra Lapiha, Ky Nguyen, and David Naccache. "The eleventh power residue symbol". In: *Journal of Mathematical Cryptology* 15.1 (2020), pp. 111–122. DOI: 10.1515/jmc-2020-0077.

[13] Ernst E. Kummer. "Allgemeine Reziprozitätsgesetze für beliebig hohe Potenzreste". In: *Monatsberichte der Königlichen Preußischen Akademie der Wissenschaften zu Berlin* (1850). Reprinted in [24, pages 345–357], pp. 154–165.

[14] Franz Lemmermeyer. "The Euclidean algorithm in algebraic number fields". In: *Expositiones Mathematicæ* 13.5 (1995). Updated version, 2 14, 2004, pp. 385–416. URL: http://www.rzuser.uni-heidelberg.de/~hb3/publ/survey.pdf.

[15] Franz Lemmermeyer. *Reciprocity Laws: From Euler to Eisenstein*. Springer Monographs in Mathematics. Springer, 2000. DOI: 10.1007/978-3-662-12893-0.

[16] Hendrik W. Lenstra, Jr. "Euclid's algorithm in cyclotomic fields". In: *Journal of the London Mathematical Society (2)* 10.4 (1975), pp. 457–465. DOI: 10.1112/jlms/s2-10.4.457.

[17] Robert George McKenzie. "The ring of cyclotomic integers of modulus thirteen is norm-Euclidean". PhD thesis. Michigan State University, 1988. DOI: 10.25335/M5NC5SP04.

[18] Jean Monnerat and Serge Vaudenay. "Short undeniable signatures based on group homomorphisms". In: *Journal of Cryptology* 24.3 (2011), pp. 545–587. DOI: 10.1007/s00145-010-9070-1.

[19] T. Ojala. "Euclid's algorithm in the cyclotomic field $\mathbb{Q}(\zeta_{16})$". In: *Mathematics of Computation* 31.137 (1977), pp. 268–273. DOI: 10.1090/S0025-5718-1977-0422202-6.

[20] Paulo Ribenboim. *13 Lectures on Fermat's Last Theorem*. Springer-Verlag, 1979. DOI: 10.1007/978-1-4684-9342-9.

[21] Renate Scheidler. "A public-key cryptosystem using purely cubic fields". In: *Journal of Cryptology* 11.2 (1998), pp. 109–124. DOI: 10.1007/s001459900038.

[22] Renate Scheidler and Hugh C. Williams. "A public-key cryptosystem utilizing cyclotomic fields". In: *Designs, Codes and Cryptography* 6.2 (1995), pp. 117–131. DOI: 10.1007/BF01398010.

[23] Lawrence C. Washington. "Units of irregular cyclotomic fields". In: *Illinois Journal of Mathematics* 23.4 (1976), pp. 635–647.

[24] André Weil, ed. *Ernst Eduard Kummer: Collected Papers I—Contributions to Number Theory*. Springer-Verlag, 1975.

[25] André Weilert. "Fast computation of the biquadratic residue symbol". In: *Journal of Number Theory* 96.1 (2002), pp. 133–151. DOI: 10.1006/jnth.2002.2783.

[26] Hugh C. Williams. "An M^3 public-key encryption scheme". In: *Advances in Cryptology – CRYPTO '85*. Ed. by H. C. Williams. Vol. 218. Lecture Notes in Computer Science. Springer, 1986, pp. 358–368. DOI: 10.1007/3-540-39799-X_26.

A COMPUTING NINTH RESIDUE SYMBOLS

A.1 COMMENTED CODE

We use in this section the following conventions: $\perp$ denotes failure, $\lfloor x \rceil$ consists in rounding x arithmetically, and if $P(\zeta)$ be a polynomial in the variable ζ we denote:

- by P_χ the reduction of P modulo the polynomial $\chi(\zeta) = 1 + \zeta^3 + \zeta^6$;
- by $P[\![\ell]\!]$ the polynomial P in which ζ was replaced by ℓ. ℓ may be a polynomial in ζ or any other expression;
- by f_c and f_n the following functions:

$$f_c[P] = (P[\![\zeta^2]\!] \cdot P[\![\zeta^4]\!] \cdot P[\![\zeta^5]\!] \cdot P[\![\zeta^7]\!] \cdot P[\![\zeta^8]\!])_\chi,$$
$$f_n[P] = (P \cdot f_c[P])_\chi.$$

The function $\texttt{Random}_L$ generates a random integer comprised between -10^L and 10^L. In the code we set $L = 27$ for the sake of the example to generate numbers $\in [-10^{27}, 10^{27}]$. The function `CoefficientList` returns all the coefficients of ζ^i up to the indicated index $\ell \leqslant u$, i.e.:

$$\texttt{CoefficientList}_\ell \left[\sum_{i=0}^{u} \epsilon_i \zeta^i \right] = \{\epsilon_0, \dots, \epsilon_\ell\}.$$

This section will make use of matrices T and U defined in Section 6.

We implement both the algorithm and test test functions to experiment with it. The following auxiliary function generates a random prime in the cyclotomic field which is 1 mod ω.

```
Function FieldRandomPrime[]
    p = 1
    While[p is composite,
        α ← 1 + (1 − ζ) Σ_{i=0}^{5} ζ^i · Random_L
        p ← f_n[α]
    ]
    Return[α_χ]
```

The following function computes 9th power residues for prime elements β and checks the result to validate the algorithm.

```
Function Resid[α,β]
    n ← f_n[β]
    γ ← f_c[β]
    q ← (α^{(n−1)/9})_χ mod n
    If ∃0 ⩽ e ⩽ 8 s.t. ((q − ζ^e)γ)_χ mod n ≡ 0 then
        Return[e]
    else
        Return[⊥]
```

Euclidean division is computed by the following function:

```
Function Euclid[α,β]
    s ← {−ζ^8, ..., −ζ, −1, 0, 1, ζ, ···, ζ^8}
    q ← ((α·f_c[β]) / f_n[β])_χ
    {c_0, ..., c_5} ← CoefficientList_5[ζ^6 + q]
    r ← Σ_{i=0}^{5} ⌊c_i⌉ ζ^i
    construct the list z ← {f_n(q − r + s_j)}_{1⩽j⩽19}
    w ← arg min_i z[i]
    r ← r − s_w
    Return[(α − rβ)_χ]
```

As its name indicates, `OmegaExp` computes the ω expansion of α up to ω^{15} :

```
Function OmegaExp[α]
    v ← {0}^16
    η ← α
    For[ℓ = 1, ℓ ⩽ 15, ℓ++,
        While[f_n[η − 1] mod 3^{ℓ+1} > 0,
            η ← (η(1 + (1 − ζ)^ℓ))_χ
            v_ℓ ++
        ]
    ]
    Return[v]
```

The rest of the code tests the algorithm. In the `(* Additional laws *)` section we generate a random prime α (renamed A for the sake of easier reference) and print it. We then print:

$$\texttt{Resid}[\zeta, \alpha], \texttt{Resid}[1+\zeta, \alpha], \texttt{Resid}[1+\zeta^2, \alpha], \texttt{Resid}[1-\zeta, \alpha]$$

compute $v = \texttt{OmegaExp}[\alpha]$ and display the value of:

$$-\sum_{i=1}^{15} v_i \pi_i \bmod 9$$

to visually check that results agree.

In the `(* Reciprocity with prime elements *)` section we generate and print two random primes α, β (again, denoted A, B in the code for easier reference). Here we check visually that primality and coupling results agree, namely that:

$$(\texttt{Resid}[\alpha, \beta] - \texttt{Resid}[\beta, \alpha]) \bmod 9 \equiv \texttt{OmegaExp}[\alpha].T.\texttt{OmegaExp}[\beta]$$

In the `(* Reciprocity with composite elements *)` section we generate five random primes $\alpha_1, \alpha_2, \alpha_3$ and β_1, β_2. We let: $\alpha = (\alpha_1\alpha_2\alpha_3)_\chi$ and $\beta = (\beta_1\beta_2)_\chi$. The test here consists in visually testing the equality:

$$\sum_{x=1}^{3}\sum_{y=1}^{2}(\texttt{Resid}[\alpha_x, \beta_y] - \texttt{Resid}[\beta_y, \alpha_x]) \bmod 9 \equiv \texttt{OmegaExp}[\alpha].T.\texttt{OmegaExp}[\beta]$$

The code then randomly refreshes $\alpha_1, \alpha_2, \alpha_3$ and β_1, β_2. We let again: $\alpha = (\alpha_1\alpha_2\alpha_3)_\chi$ and $\beta = (\beta_1\beta_2)_\chi$. The program prints for visual inspection the value:

$$\sum_{x=1}^{3}\sum_{y=1}^{2}\texttt{Resid}[\alpha_x, \beta_y] \bmod 9$$

Let $w = 0$ and $\gamma = \alpha$. We instruct the computer to dynamically update on the screen the value of $f_n(\gamma)$ and perform the following operations:

```
While[fn(γ) > 1,
    w ← w + OmegaExp[α].T.OmegaExp[β]
    {α, β} ← {β, α}
    γ ← Euclid[α, β]
      While[fn[γ] mod 3 ≡ 0,
        γ ← ((γ·fc[1−ζ])/3)χ
        w ← w − π4.OmegaExp[β] mod 9
      ]
    If[γ(1) mod 3 ≡ 2,  γ ← −γ]
    α ← γ
]
```

Finally, we print the value of the symbol, $\texttt{OmegaExp}[\alpha].T.\texttt{OmegaExp}[\beta] \bmod 9$.

A.2 SOURCE CODE

```
(* Defining cyclotomic field and norm function *)
PR[α_,n_:0] := PolynomialRemainder[α,1+ζ^3+ζ^6,ζ,Modulus→n];
fC[α_]      := PR[(α/.ζ → ζ^2)(α/.ζ → ζ^4)(α/.ζ → ζ^5)(α/.ζ → ζ^7)(α/.ζ → ζ^8)];
fN[α_]      := PR[α fC[α]];

(* Generates a random prime in the cyclotomic field, which is 1 mod ω *)
FieldRandomPrime[] := Module[{α,p,L},
    {p,L}={1,27};
    While[!PrimeQ[p],
        α=1+(1-ζ) Sum[RandomInteger[{-10^L,10^L}]ζ^i,{i,0,5}];
        p=fN[α];];
    Return[PR[α]];
];

(* Computing ninth power residue in the case where β is a prime element *)

PolyExp := If[#2==0,1,PR[#0[PR[#1^2,#3],Floor[#2/2],#3] #1^Mod[#2,2],#3]]&[#1,#2,#3]&;
```

```
Resid[α_,β_] := Module[{n,γ,q,e},
    {n,γ}={fN[β],fC[β]};
    q=PolyExp[α,(n-1)/9,n];
    For[e=0,e⩽8,e++,
        If[PR[(q-ζ^e)γ,n]==0,Return[e]];
    ];
    Return["This should not happen!"];
];

(* Euclidean division - Not proven *)
s = Union[q=Table[ζ^i,{i,0,8}],-q,{0}];

Euclid[α_,β_] := Module[{q,r,z,w},
    q = PR[α fC[β]/fN[β]];
    r = Round[Delete[CoefficientList[ζ^6+q,ζ],-1]].Table[ζ^i,{i,0,5}];
    z = fN/@(q-r+s);
    w = Position[z,Min[z]][[1,1]];
    r = r-s[[w]];
    Return[PR[α-r β]];
];

(* Compute ω-expansion of α up to ω^15 *)
OmegaExp[α_] := Module[{v,l,η},
    v = ConstantArray[0,15];
    η = α;
    For[l=1,l⩽15,l++,
        While[Mod[fN[η-1],3^(l+1)]>0,
            η = PR[η(1+(1-ζ^l))];
            v[[l]]++;
        ];
    ];
    Return[v];
];

     ⎛ 0 5 3 7 1 8 7 5 3 6 3 3 6 3 0 ⎞            ⎛ 8 6 1 0 ⎞
     ⎜ 4 0 4 3 2 3 1 6 6 3 3 0 6 0 0 ⎟            ⎜ 4 6 7 0 ⎟
     ⎜ 6 5 0 6 0 6 0 0 0 0 0 0 0 0 0 ⎟            ⎜ 8 6 1 0 ⎟
     ⎜ 2 6 3 0 5 0 6 6 0 0 3 0 0 0 0 ⎟            ⎜ 5 4 3 0 ⎟
     ⎜ 8 7 0 4 0 0 3 0 0 6 0 0 0 0 0 ⎟            ⎜ 1 7 7 0 ⎟
     ⎜ 1 6 3 0 0 0 0 0 0 0 0 0 0 0 0 ⎟            ⎜ 7 8 7 6 ⎟
     ⎜ 2 8 0 3 6 0 0 3 0 0 0 0 0 0 0 ⎟            ⎜ 7 4 6 0 ⎟
T =  ⎜ 4 3 0 3 0 0 6 0 0 0 0 0 0 0 0 ⎟;    U =    ⎜ 1 2 7 0 ⎟;
     ⎜ 6 3 0 0 0 0 0 0 0 0 0 0 0 0 0 ⎟            ⎜ 0 3 3 8 ⎟
     ⎜ 3 6 0 0 3 0 0 0 0 0 0 0 0 0 0 ⎟            ⎜ 0 6 3 0 ⎟
     ⎜ 6 6 0 6 0 0 0 0 0 0 0 0 0 0 0 ⎟            ⎜ 0 3 0 0 ⎟
     ⎜ 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 ⎟            ⎜ 6 3 6 6 ⎟
     ⎜ 3 3 0 0 0 0 0 0 0 0 0 0 0 0 0 ⎟            ⎜ 6 6 0 0 ⎟
     ⎜ 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 ⎟            ⎜ 6 3 6 0 ⎟
     ⎝ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 ⎠            ⎝ 0 0 0 3 ⎠

(* Additional laws *)
Print["α = ",A=FieldRandomPrime[]];
Print["Using primality: ",Resid[#,A]&/@ {ζ,1+ζ,1+ζ^2,1-ζ}];
v=OmegaExp[A];
Print["Using structure: ",Mod[-Sum[v[[i]] U[[i]],{i,1,15}],9]];

(* Reciprocity with prime elements *)
Print["{α,β}=",{A,B}=Array[FieldRandomPrime[]&,2]];
Print["Using primality: ",Mod[Resid[A,B]-Resid[B,A],9]];
Print["Using coupling : ",Mod[OmegaExp[A].T.OmegaExp[B],9]];

(* Reciprocity with composite elements *)
{α[1],α[2],α[3],β[1],β[2]}=Array[FieldRandomPrime[]&,5];
Print["{α,β}=",{A,B}=PR/@{α[1] α[2] α[3],β[1] β[2]}];
Print["Using factors  : ",Mod[Sum[Resid[α[x],β[y]]-Resid[β[y],α[x]],{x,1,3},{y,1,2}],9]];
Print["Using coupling : ",Mod[OmegaExp[A].T.OmegaExp[B],9]];
{α[1],α[2],α[3],β[1],β[2]}=Array[FieldRandomPrime[]&,5];
Print["{α,β}=",{A,B}=PR/@{α[1] α[2] α[3],β[1] β[2]}];
Print["Using factors  : ",Mod[Sum[Resid[α[x],β[y]],{x,1,3},{y,1,2}],9]];
```

```
{w,γ}={0,A};
Print["Norm : ",Dynamic[fN[γ]]];

While[fN[A]>1,
    (* Invert α and β *)
    w = Mod[w+OmegaExp[A].T.OmegaExp[B],9];
    {A,B} = {B,A};

    (* Reduce α mod β *)
    γ = Euclid[A,B];
    While[Mod[fN[γ],3]==0,
        γ = PR[γ fC[1-ζ]/3];
        w = Mod[w-((#[[4]])&/@ U).OmegaExp[B],9];
    ];

    If[Mod[(γ/.ζ →1),3]==2,γ = -γ];
    A = γ;
];

Print["Algorithm : ", Mod[OmegaExp[A].T.OmegaExp[B],9]];
```